NASCIO
Representing Chief Information
Officers of the States

August 2, 2017

Submitted via email at: cybersecurityworkforce@nist.gov

Kevin Kimball
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: Cybersecurity Workforce RFI

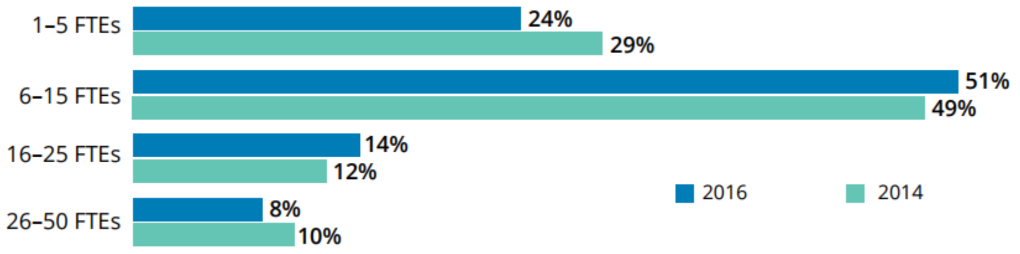
Dear Mr. Kimball,

On behalf of the National Association of State Chief Information Officers (NASCIO), thank you for the opportunity to provide comments in response to the Request for Information (RFI), "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development."

NASCIO represents the state chief information officers (CIO) and information technology executives and managers from the states, territories and D.C. State CIOs are leaders of state information technology policy and implementation and continually look for opportunities to improve operations, bring innovation, and transform state government through technological solutions. Naturally, cybersecurity has been a top priority for state CIOs for the past several years (See, NASCIO Top Ten Policy and Technology Priorities Survey, 2013-2016). As such, ensuring a cybersecurity workforce that can meet the needs of state government is a related priority that is top of mind for state CIOs.

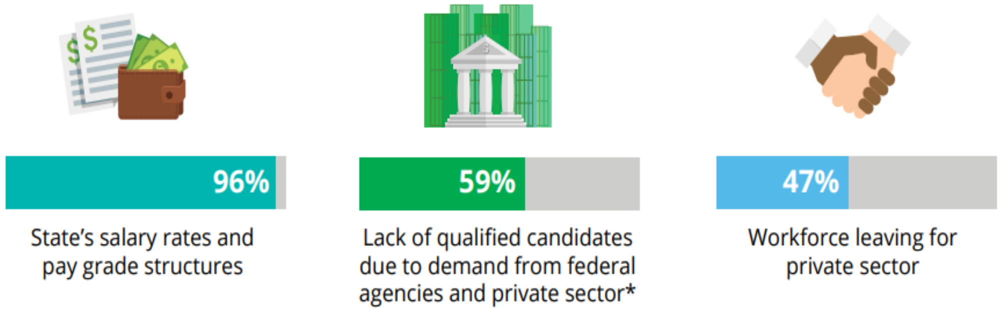
In our comments, we will largely address the cybersecurity workforce challenges that face state government, current recruitment and retention practices, and offer recommendations that could aid in the ability of state government to make efficient use of existing human resources.

In the 2016 Deloitte-NASCIO Cybersecurity Study, we evaluated the survey responses from 49 state chief information security officers (CISOs) regarding a variety of cybersecurity issues, including the workforce. Currently, the majority of states have enterprise cybersecurity teams between 6-15 full-time equivalents (FTEs) and overall team sizes show a small increase year after year (see chart below). While the cybersecurity workforce may be increasing, the shortage of security professionals continues to pose a challenge to addressing state cybersecurity; this was ranked the second most concerning



Source: 2014 and 2016 Deloitte-NASCIO Cybersecurity Studies.

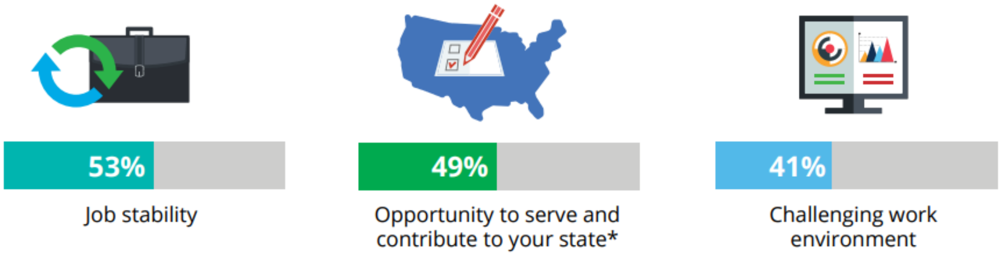
Graphic: Deloitte University Press | DUPress.com challenge (51 percent) for state CISOs. In a 2015 NASCIO study, "State IT Workforce: Facing Reality with Innovation," 67 percent of state CIOs reported that security was the discipline that presented the greatest challenge in attracting and retaining IT employees. Specific to the cybersecurity workforce, 96 percent of state CISOs find "state's salary rates and pay grade structures" as the factor that poses the biggest challenge to the state's ability to develop, support, and maintain a cybersecurity workforce.



*New in 2016
Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

While these challenges are expected to persist, state governments are utilizing government-unique benefits such as the "opportunity to serve and contribute to your state" to attract and recruit cybersecurity talent (see chart below). Data from "State IT Workforce: Facing Reality with Innovation," also show that more than 50 percent of state CIOs used social media, promoted non-salary benefits (e.g. stability), utilized college placement systems, created internships, and converted contractors to state employees to attract and retain a qualified IT workforce. When state CIOs were asked about what attracts IT employees to work for the state, they responded: benefits package (76 percent), job stability (72 percent), pension/retirement plan (60 percent) among others.



*New in 2016
Source: 2016 Deloitte-NASCIO Cybersecurity Study.

Graphic: Deloitte University Press | DUPress.com

The State of Washington serves as a great example of how state governments are adapting to the increasingly competitive nature of attracting qualified IT and security professionals. In Washington, half of the government workforce was eligible to retire between 2014-2019. The State is also home to "brand name" technology companies like Microsoft, Amazon, Apple, and others which created a difficult environment for Washington Technology Solutions (WaTech), the state's consolidated technology agency to attract and retain qualified IT and security personnel. In light of these challenges, WaTech implemented the "Technology Employer of Choice" initiative which employs a variety of methods to attract and retain technology talent, these include:

- Experimenting with self-management (Holacracy)
- Piloting physical space changes
- Reclassifying state government technology jobs
- Hiring for value alignment instead of skills
- Finding top talent in innovative ways including participation in local college and university curriculum boards and implementing a work-internship program

After a one-year holacracy pilot, which replaces traditional hierarchical governance with one that organizes work instead of people, WaTech employees reported feeling more empowered and the organization made decisions and took action ten times faster.

WaTech is also finding top talent in innovative ways. WaTech's participation in local college and university curriculum boards ensure that students are learning contemporary skills and practices. It also recruits through a work-internship program for students and veterans. 26 percent of interns are veterans and of 56 interns, 64 percent have become state technology employees.

In response to common challenges like salary and pay grades that are not competitive with the private sector, WaTech is restructuring their IT classification system to better align with technology job functions in the industry and provide managers with more flexibility for compensating highly desirable skills. In 2015, job families such as "software development and database administration" were identified and agencies began filling out new position descriptions based on newly developed job families. Once fully in place, the state will be able to perform job analysis and obtain more accurate compensation comparisons in the technology sector. Read more about Washington's reclassification for IT positions here.

Like WaTech, states are employing and developing innovative hiring practices and policies to hire much-needed IT and cybersecurity professionals. However, state CIOs acknowledge the ongoing difficulties in achieving optimal levels of a cybersecurity workforce within state government and would recommend that our federal partners work with state CIOs to enable more efficient use of existing human resources.

NASCIO has long advocated for the harmonization of federal cybersecurity regulations and normalization of the audit process as way to not only strengthen the cybersecurity posture of states but also better utilize the existing cybersecurity workforce within state government. Federal cybersecurity regulations such as IRS Publication 1075, FBI-Criminal Justice Information Services (CJIS), the Health Insurance Portability and Protection Act (HIPPA), CMS Minimum Acceptable Risk for Exchanges (MARS-E) among others are just some of the regulations with which state governments must comply. Federal cybersecurity regulations typically address common security topics such as access control, security training, audit logs etc. but differ in their specific requirements without a sufficient policy justification. This is despite that fact that all parties can agree that the information federal regulations seek to protect is "high-risk" and must be guarded at a level commensurate with that risk.

As states CIOs and CISOs attempt to digest and comply with voluminous and disparate federal regulations, they are finding that an inordinate amount of human resources is being invested on compliance activity rather than actions that would enhance the security posture of the state. Consider the experience of the State of Maine; they spent 4,000 hours on compliance activity for one IRS audit (see chart below). Maine's investment in federal compliance is not unique and many states have shared that they, too, face similar challenges addressing federal compliance requirements. Please see our written testimony to the Senate Homeland Security and Governmental Affairs Committee for more examples of how disparate federal cybersecurity regulations impact state governments' cybersecurity workforce.

Regulatory Agency	State FTEs	Total Hours
Internal Revenue Service (IRS)	12+	4,000
Social Security Administration (SSA)	4+	2,500
U.S. Treasury	1	60
Health Insurance Portability and Accountability Act (HIPAA)	6+	800
Criminal Justice Information Service (CJIS)	3+	800
Centers for Medicare and Medicaid Services (CMS)	12+	3,000
Total		**11,160**

State CIOs recognize that recruiting and retaining qualified cybersecurity personnel will continue to be challenging. The federal government can assist states mitigate the impact of the cybersecurity workforce shortage by enabling more efficient, focused use of existing human resources. We believe this can be achieved through harmonization of disparate federal cybersecurity regulations and normalizing the federal audit process. NASCIO has begun discussion with the appropriate regulating agencies and will continue to advocate for a more efficient regulatory regime. We would also recommend that the federal government consider establishing a working group to study and collectively develop a viable solution to this issue.

We appreciate the opportunity to offer comments on the cybersecurity workforce challenges that face state government, current recruitment and retention strategies, and recommendations for the efficient use of existing cybersecurity personnel. State CIOs appreciate the mission to secure public networks and information and look forward to the recommendations and guidance offered through this RFI. If you have any questions, please contact NASCIO director of government affairs Yejin Cooke at ycooke@NASCIO.org or 202.624.8477.

Sincerely,

Mark Raymond
President, NASCIO
Chief Information Officer, State of Connecticut

Doug Robinson
Executive Director, NASCIO